National Infrastructure Protection Center CyberNotes

Issue #2001-05

March 12, 2001

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between February 19 and March 8, 2001. The table provides the vendor/operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear as red and/or italic text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
APC[1]	Multiple	Web/SNMP Management Card Firmware 3.0 and previous	Several remote Denial of Service vulnerabilities exist due to a lockout delay and the restriction of allowing only one simultaneous Telnet connection.	Upgrade available at: http://www.apc.com/tools/download/	APC Telnet Administration Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Atrium Software[2]	Windows 95/98/NT 2000	Mercur Mail Server 3.3	An unchecked buffer vulnerability exists in the EXPN command, which could let a remote malicious user cause a Denial of Service or execute arbitrary code.	No workaround or patch available at time of publishing.	Mercur Mail Server EXPN Buffer Overflow	Low/**High**	Bug discussed in newsgroups and websites. Exploit script has been published.

[1] Securiteam, February 28, 2001.

[2] Securiteam, March 3, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Centrinity[3]	Windows NT	FirstClass 5.50	A vulnerability exists which could let a remote malicious user connect to the system on port 25 and send mail appearing to the users of the first-class system as coming from a local user on the server, including a privileged user.	No workaround or patch available at time of publishing.	FirstClass Local User Mail Spoofing	Medium	Bug discussed in newsgroups and websites.
ChiliSoft[4]	Unix	Chili!Soft ASP for Linux 3.0, 3.5, 3.5.2	Several vulnerabilities exist: a remote malicious user could potentially view sensitive information and take control of the server; a default username and password are used for the administrative console if auto-detect setting options are used; and there are several file permission vulnerabilities. These vulnerabilities could lead to a root compromise.	No workaround or patch available at time of publishing.	Chili!Soft Multiple Vulnerabilities	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
ChiliSoft[5]	Unix	Chili!Soft ASP for Linux 3.0, 3.5, 3.5.2	A Denial of Service vulnerability exists due to the fact that the web-based license update tool creates its server license file as world-writeable. As a result, a malicious user may overwrite, delete or modify the file.	No workaround or patch available at time of publishing.	Chili!Soft License File Deletion Denial of Service	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Cisco[6]		IOS software releases based on versions 11.x and the 12.0 interface	Several vulnerabilities exist involving the creation and exposure of SNMP community strings, which could let a remote malicious user change configuration objects within the MIB-II Community, rename the system, change the location name in the system, and/or change the contact information for the system.	Upgrade available at: http://www.cisco.com	Cisco IOS ILMI SNMP Community String	Medium	Bug discussed in newsgroups and websites. Vulnerability has appeared in the Press and other public media.
Datawizard Technologies, Inc.[7]	Windows 95/98/98se/ NT 4.0/2000	FtpXQ 2.0.93	A directory traversal vulnerability exists which could let a malicious user gain sensitive information, including password files.	No workaround or patch available at time of publishing.	FtpXQ Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Dattaraj Rao[8]	Multiple	Simple Server 1.0	A directory traversal vulnerability exists which could let a remote malicious user gain read access to directories and files outside the root directory.	No workaround or patch available at time of publishing.	Simple Server Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[3] Bugtraq, February 21, 2001.
[4] Securiteam, February 25, 2001.
[5] Bugtraq, February 27, 2001.
[6] Cisco Security Advisory, CI-01.02, February 27, 2001.
[7] Securiteam, March 5, 2001.
[8] Securiteam, March 3, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Elm Development Group[9]	Multiple	ELM 2.5.3	A buffer overflow vulnerability exists in the –f command option, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Elm Alternative Folder Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit scripts has been published.
Francisco Burzi[10]	Multiple	PHP-Nuke 4.3	Security vulnerabilities exist which could allow a remote malicious user execute arbitrary commands, change administrative passwords, and gain administrator privileges.	PHP-Nuke version 4.4.1 has been released.	PHP Nuke User Settings Modification and Administrator Account Compromise	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Guido Frassetto[11]	Windows 95/98/NT 3.5.1/4.0/ 2000	SEDUM HTTP Server 2.1	A remote Denial of Service vulnerability exists when a large number of characters are submitted to the webserver.	No workaround or patch available at time of publishing.	SEDUM HTTP Webserver Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Headlight Software[12]	Windows 98/98/ME/ NT 3.5.1/4.0 2000	My Getright 1.0b1-1.0b4	Two vulnerabilities exist which could allow a remote malicious user to upload and overwrite existing files or cause a Denial of Service	Upgrade available at: http://www.mygetright.com/	My Getright Remote Arbitrary File Overwrite and Denial of Service	Low/ Medium	Bug discussed in newsgroups and websites.
Hewlett Packard[13]	Unix	HP9000 Series 700/800 running HP-UX releases 10.01, 10.10, 10.20, 11.00	A Denial of Service vulnerability exists in the HP-UX Software Distributor.	No workaround or patch available at time of publishing.	HP-UX Software Distributor Denial of Service	Low	Bug discussed in newsgroups and websites.
Hewlett-Packard[14]	Unix	HP3000 running MPE/iX release 5.5, 6.0, 6.5	A vulnerability exists in the MPE/iX linkeditor and NM debug that could let a malicious user gain privileged access.	No workaround or patch available at time of publishing.	Hewlett-Packard MPE/iX linkeditor and NM debug	Medium	Bug discussed in newsgroups and websites.
Holger Lamm[15]	Unix	PGP4pine 1.75.6	A vulnerability exists due to a failure to properly identify expired keys when working with the Gnu Privacy Guard (GnuPG) program, which could result in the transmission of sensitive information in clear text.	No workaround or patch available at time of publishing.	PGP4pine Encryption Failure	Medium	Bug discussed in newsgroups and websites.
Infopop[16]	Unix	Ultimate Bulletin Board 5.0.x Beta	A vulnerability exists due to insufficient checking of bulletin board input, which could let a remote user execute malicious code.	Upgrade available at: http://www.infopop.com/nonbusiness/nonbusiness_ubb.html	Ultimate Bulletin Board Tag Javascript Embedding	**High**	Bug discussed in newsgroups and websites.

[9] Securiteam, February 28, 2001.
[10] Argentinian Security Group, March 2, 2001.
[11] Bugtraq, February 23, 2001.
[12] Strumpf Noir Society Advisories, February 26, 2001.
[13] eSecurityOnline Free Vulnerability Alert 3429, March 1, 2001.
[14] eSecurityOnline Free Vulnerability Alert 3409, February 21, 2001.
[15] CryptNET Security Advisory, February 20, 2001.
[16] Bugtraq, February 21, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Jarle Aase[17]	Windows 95/98/NT 4.0/2000	War FTPD 1.67b04	A directory traversal vulnerability exists which could let a remote malicious user gain read access to files residing on the target machine.	Upgrade available at: ftp://ftp.jgaa.com/pub/products/Windows/WarFtpDaemon/1.6_Series/ward167-5.zip	Jarle Aase War FTPD Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft[18]	Windows 2000	Internet Information Services (IIS) 5.0	A Denial of Service vulnerability exists if WebDav is enabled and a specially crafted request is sent.	Frequently asked questions regarding this vulnerability and the workaround can be found at: http://www.microsoft.com/technet/security/bulletin/MS01-016.asp	IIS Malformed WebDAV Request CVE name: CAN-2001-0151		Bug discussed in newsgroups and websites. Exploit script has been published.
Microsoft[19]	Windows 2000	Windows 2000 Professional, 2000 Server, 2000 Advanced Server, 2000 Datacenter Server	An unchecked vulnerability exists in the event viewer, which could let a malicious user execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/ms01-013.asp	Windows 2000 Event Viewer Unchecked Buffer	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the Press and other public media.
Microsoft[20]	Windows 95/98/NT 4.0/2000	Internet Explorer 5.01, 5.5; Windows Scripting Host 5.1, 5.5	A vulnerability exists in IE and Windows Scripting Host that could let a malicious user execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/MS01-015.asp Three other vulnerabilities also are eliminated by this patch: A variant of the "Frame Domain Verification" vulnerability discussed in Microsoft Security Bulletins MS00-033, MS00-055, and MS00-093; a vulnerability that is identical in effect to the "Frame Domain Verification" vulnerability; and a vulnerability that affects how Telnet sessions are invoked via IE.	Internet Explorer and Windows Scripting Host Cached Location CVE name: CAN-2001-0002	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[17] Bugtraq, March 6, 2001.
[18] Microsoft Security Bulletin, MS01-016, March 8, 2001.
[19] Microsoft Security Bulletin, MS01-013, February 26, 2001.
[20] Microsoft Security Bulletin, MS01-015, March 6, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[21]	Windows NT 2000	Exchange Server 2000, Internet Information Services (IIS) 5.0	A Denial of Service vulnerability exists due to the way web client requests are handled.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/MS01-014.asp	Microsoft Malformed URL Denial of Service CVE name: CAN-2001-0146	Low	Bug discussed in newsgroups and websites.
Microsoft[22] ***Exploit script released[23]***	**Windows NT 4.0**	**Windows NT 4.0; Windows NT 4.0 Terminal Server Edition**	**A Denial of Service vulnerability exists due to inappropriate permissions applied to a networking mutex.**	**Frequently asked questions regarding this vulnerability and the patch can be found at:** **http://www.microsoft.com/technet/security/bulletin/fq01-003.asp**	**Windows NT Winsock Mutex Denial of Service**	**Low**	**Bug discussed in newsgroups and websites.** ***Exploit script has been published.***
Mobydisk[24]	Windows 95/98/NT	Moby Netsuite 1.0	A Denial of Service vulnerability exists when large HTTP requests are submitted, which could allow a remote malicious user to execute arbitrary code.	No workaround or patch available at time of publishing.	Moby Netsuite Remote Denial of Service	High	Bug discussed in newsgroups and websites. Exploit has been published.
Multiple Vendors[25]	Unix	Joseph Allen joe 2.8; Red Hat Linux 5.2, 6.x and 7; Linux-Mandrake 6.0, 6.1, 7.0, 7.1, 7.2, Corporate Server 1.0.1; Debian GNU/Linux 2.2	A vulnerability exists in the .joerc file, which could let a malicious user execute arbitrary commands.	<u>**RedHat:**</u> ftp://updates.redhat.com <u>**Linux-Mandrake:**</u> http://www.linux-mandrake.com/en/ftp.php3 <u>**Debian:**</u> http://security.debian.org/dists/stable/updates/main/	Joe Text Editor .joerc Arbitrary Command Execution	High	Bug discussed in newsgroups and websites. Exploit has been published.
Multiple Vendors[26] ***Exploit script released[27]***	**Unix**	**SSH Communications SSH 1.2.24-1.2.31; OpenSSH 1.2.2, 1.2.3, 2.1, 2.1.1, 2.2**	**Various SSH implementations are vulnerable to a buffer overflow, which could allow a remote malicious user to execute arbitrary code.**	**Patches available at:** <u>**OpenSSH:**</u> **ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH/openssh-2.3.0.tgz** <u>**SSH Communications:**</u> **ftp://ftp.ssh.com/pub/ssh/ssh-2.4.0.tar.gz** <u>**Debian:**</u> **http://security.debian.org/dists/stable/updates/main/**	**SSH CRC-32 Compensation Attack Detector** **CVE name: CAN-2001-0144**	**High**	**Bug discussed in newsgroups and websites. Exploit has been published.** ***Exploit script has been published.***

[21] Microsoft Security Bulletin, MS01-014, March 1, 2001.
[22] Microsoft Security Bulletin, MS01-003, January 25, 2001.
[23] Securiteam, March 6, 2001.
[24] Bugtraq, February 9, 2001.
[25] Bugtraq, February 28, 2001.
[26] eSecurityOnline Free Vulnerability Alert 3388, February 12, 2001.
[27] Securiteam, March 4, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[28, 29, 30]	Unix	Zope 2.3.1 b1 & prior	Multiple vulnerabilities exist: users can use through-the-web scripting capabilities to view and assign class attributes to ZClasses, possibly allowing them to make inappropriate changes; and there are security problems with the ObjectManager, PropertyManager and PropertySheet classes.	**RedHat:** ftp://updates.redhat.com/powertools **Linux-Mandrake:** http://www.linux-mandrake.com/en/ftp.php3 **Conectiva Linux:** ftp://atualizacoes.conectiva.com.br/ **FreeBSD:** ftp://ftp.FreeBSD.org/pub/FreeBSD/ports	Multiple Zope Vulnerabilities	Medium	Bug discussed in newsgroups and websites.
Multiple Vendors[31, 32, 33, 34]	Unix	Linux-Mandrake 7.1, 7.2, Corporate Server 1.0.1; Immunix OS 7.0-beta and 7.0; Conectiva Linux 4.0, 4.0es, 4.1, 4.2, 5.0, prg gráficos, ecommerce, 5.1, 6.0; Debian GNU/Linux 2.2; Slackware 7.1, current	A buffer overflow vulnerability exists in the sudo program, which could let a malicious user gain root privileges.	**Linux-Mandrake:** http://www.linux-mandrake.com/en/ftp.php3 **Immunix:** http://immunix.org/ImmunixOS/7.0/updates/RPMS/sudo-1.6.3p6-1_imnx_1.i386.rpm **Conectiva:** ftp://atualizacoes.conectiva.com.br/ **Debian:** http://security.debian.org/dists/stable/updates/ **Slackware:** ftp://ftp.slackware.com/pub/slackware/	Sudo Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Netscape[35]	Windows NT	Netscape Directory Server 4.1, 4.12	A buffer overflow vulnerability exists when a specially crafted query is sent to the server, which could let a malicious user cause a Denial of Service or execute arbitrary code.	No workaround or patch available at time of publishing.	Netscape Directory Server Buffer Overflow CVE name: CAN-2001-0164	**High**	Bug discussed in newsgroups and websites.
Netscape[36]	Windows NT	Netscape Collabra Server 3.5.4	A Denial of Service vulnerability exists if invalid input is submitted repeatedly to ports 5238 and 5239.	No workaround or patch available at time of publishing.	Netscape Collabra Malformed Data and Memory Leak Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.

[28] Red Hat, Inc. Red Hat Security Advisory, RHSA-2001:021-06, February 26, 2001.
[29] Linux-Mandrake Security Update Advisory, MDKSA-2001:025, February 26, 2001.
[30] Conectiva Linux Security Announcement, CLA-2001:382, March 2, 2001.
[31] Linux-Mandrake Security Update Advisory, MDKSA-2001:024, February 26, 2001.
[32] Immunix OS Security Advisory, IMNX-2001-70-004-01, February 26, 2001.
[33] Conectiva Linux Security Announcement, CLA-2001:381, February 26, 2001.
[34] Debian Security Advisory, DSA-031-2, March 6, 2001.
[35] @stake, Inc. Security Advisory Notification, A030701-1, March 7, 2001.
[36] Defcom Labs Advisory, def-2001-08, February 26, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Netwin[37]	Windows 98/NT 4.0/2000, Unix	SurgeFTP 1.0b	A remote Denial of Service vulnerability exists due to a design flaw.	Upgrade available at : **NetWin upgrade SurgeFTP NT 1.1h:** ftp://ftp.netwinsite.com/pub/surgeftp/surgeftp11h_nt.exe **NetWin upgrade SurgeFTP Linux 1.1h:** ftp://ftp.netwinsite.com/pub/surgeftp/surgeftp11h_linux.tar.gz	SurgeFTP Malformed Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Oracle[38] ***Upgrade now available[39]***	**Windows NT 2000**	**Oracle8 8.1.7**	**A vulnerability exists in the way input is handled by the JSP agent which could let a remote malicious user execute arbitrary .jsp files.**	*Upgrade available at:* *http://otn.oracle.com/*	**Oracle JSP/SQLJSP Servlet Execution**	**High**	**Bug discussed in newsgroups and websites.**
Orange Software[40]	Windows 94/98ME/ NT 4.0/2000	Orange Web Server 2.1	A remote Denial of Service vulnerability exists when a specially crafted GET request is sent via a Telnet connection.	No workaround or patch available at time of publishing.	Orange Web Server Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Palm[41]	Multiple	Palm OS 3.3, 3.5.2	A vulnerability exists in the debugging mode which could let a malicious user with physical access to the PDA bypass the unit's password protections.	No workaround or patch available at time of publishing.	Palm Debugger Password Bypass	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Rasmus J.P. Allenheim[42]	Unix	SunFTP 1.0 Build 9	A vulnerability exists which could allow remote malicious ftp users to read arbitrary system files. This could allow users to place Trojan horse programs on the system and gain control.	This ftp server does not appear to be supported anymore. It is suggested that users upgrade to a supported ftp server.	SunFTP Unauthorized File Access	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Robin Twombly[43]	Windows 95/98/NT 4.0/2000	A1 Web Server 1.0	Two vulnerabilities exist: a directory traversal vulnerability, which could let a remote malicious user gain read access to directories and files outside the web root; and a remote Denial of Service vulnerability.	No workaround or patch available at time of publishing.	A1 HTTP Server Directory Traversal and Denial of Service	Low/ Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Sapio Design Ltd.[44]	Windows 95/98/98se	WebReflex 1.55	A Denial of Service vulnerability exists when an excessively long HTTP GET request is sent to the web server, which could allow a remote malicious user to execute arbitrary code.	No workaround or patch available at time of publishing.	WebReflex GET Denial Of Service	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[37] Strumpf Noir Society Advisories, March 1, 2001.
[38] Georgi Guninski Security Advisory #36, January 22, 2001.
[39] Securiteam, February 19, 2001.
[40] Bugtraq, February 27, 2001.
[41] Securiteam, February 20, 2001.
[42] Securiteam, March 6, 2001.
[43] Securiteam, March 6, 2001.
[44] Bugtraq, February 27, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
WhitSoft Development[45]	Windows 95/98/98se/ NT 4.0/2000	SlimServe FTPd version 1.0	A directory traversal vulnerability exists which could let a remote malicious user view files and directories outside the virtual web directory.	No workaround or patch available at time of publishing.	SilmServe Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
WhitSoft Development[46]	Windows 95/98/98se/ NT 4.0/2000	SlimServe HTTPd 1.1	A remote Denial of Service vulnerability exists due to the way HTTP GET requests are handled.	No workaround or patch available at time of publishing.	SlimServe HTTPD Get Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Winzip Computing, Inc.[47]	Windows NT/2000	Winzip 8.0	A buffer overflow vulnerability exists in the /zipandemail option which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Winzip32 zipandemail Buffer Overflow	**High**	Bug discussed in newsgroups and websites.

*Risk is defined in the following manner:

High - A vulnerability that will allow an intruder to immediately gain privileged access (e.g., sysadmin, and root) to the system and/or the intruder can execute or alter arbitrary system files. An example of this would be a vulnerability in which a sequence of instructions is sent to a machine by an unauthorized user and the machine responds with a command prompt.

Medium - A vulnerability that will allow an intruder immediate access to the system that is not privileged access. This allows the intruder the opportunity to continue the attempt to gain root access. An example would be a configuration error that allows an intruder to capture the password file.

Low - A vulnerability that provides information to an intruder that could lead to further compromise attempts or a Denial-of-Service (DoS) attack. The reader should note that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered as a "High" threat.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between February 23 and March 8, 2001, listed by date of script, script names, script description, and comments. **Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing**. During this period, 19 scripts, programs, and net-news messages containing holes or exploits were identified. NOTE: At times, scripts/techniques may contain names or content that may be considered offensive.

Date of Script (Reverse Chronological Order)	Script name	Script Description
March 8, 2001	Ethereal-0.8.16.tar.gz	A GTK+-based network protocol analyzer, which allows the capture and interactive browsing of the contents of network frames.

[45] Securiteam, March 8, 2001.
[46] Bugtraq, February 28, 2001.
[47] Defcom Labs Advisory, def-2001-09, March 2, 2001.

Date of Script (Reverse Chronological Order)	Script name	Script Description
March 8, 2001	Ssh-brute.sh	A brute force password guesser that guesses the root's password without being logged.
March 8, 2001	Vv5.pl	Perl script which exploits the IIS Malformed WebDAV Request vulnerability.
March 6, 2001	Mutation.c	Script which exploits the Windows NT Winsock Mutex Denial of Service vulnerability.
March 5, 2001	Hhp-ntping_smash.c	A local root exploit for NTping.
March 5, 2001	Hhp-ospf_smash.c	A local root exploit for ospf_monitor.
March 4, 2001	Imapd_lsub.c	Remote exploit for the Red Hat overflow vulnerability in the LSUB command.
March 4, 2001	Packet.c	Script which exploits the SSH CRC-32 Compensation Attack Detector vulnerability.
March 3, 2001	**Mercur33exploit.c**	**Script which exploits the Atrium Software Mercur Mail Server 3.3 EXPN Buffer Overflow vulnerability.**
March 3, 2001	Ngrep-1.39.tar.gz	A network sniffing tool that strives to provide most of GNU grep's common features.
March 3, 2001	Rdc270201.adv.en	Exploit URL for the PHP-Nuke v4.4.1a vulnerability.
March 2, 2001	Beatlm001.zip	BeatLm searches out the password from LM/NTLM authentication information (LanManager and Windows NT challenge/response).
March 1, 2001	Elvwreck.c	Script which exploits the FreeBSD 3.5.1 and 4.2 ja-elvis and ko-helvis vulnerability.
February 28, 2001	Apcdos.pl	Script which exploits the APC Telnet Administration Denial of Service vulnerability.
February 28, 2001	**Elm253-exploit.c**	**Script which exploits the Elm Alternative -Folder Buffer Overflow vulnerability.**
February 28, 2001	**Elm-kiss.c**	**Script which exploits the Elm Alternative -Folder Buffer Overflow vulnerability.**
February 26, 2001	Ettercap-0.2.1.tar.gz	A network sniffer/interceptor/logger for switched LANs that uses ARP poisoning and the man-in-the-middle technique to sniff all the connections between two hosts.
February 26, 2001	Man-cgi.txt	Exploit URL for the Man-cgi v1.3 and v2.0 remote vulnerabilities.
February 23, 2001	Imapd_exploit.c	Script which exploits the Imapd v12.264 lsub command vulnerability.

Trends

Probes/Scans:

There has been an increase in the number of suspicious probes and scans designed to find vulnerable domain name servers on corporate networks.

Backdoor-G and NetBus Trojan scans have increased in number.

Other:

A new technique has emerged that exploits vulnerabilities in Windows machines installed with IIS 4.0 or 5.0. A Windows NT/2000 utility called "FireDaemon" is being used as a part of a toolkit to further compromise the machines. For more information, please see security advisory located at: http://www.firedaemon.com under the "Security Alert" posted on March 7, 2001.

Recent attacks against e-commerce and e-banking sites are being carried out via known vulnerabilities for which patches have been available for months or, in some cases, years. For more information, please see NIPC Advisory 01-003 located at: http://www.nipc.gov/warnings/advisories/2001/01-003.htm.

NIPC is evaluating an Internet worm by the name of "nakedwife.exe" that has been propagating in the wild. For more information, please see NIPC ADVISORY 01-002 located at: http://www.nipc.gov/warnings/advisories/2001/01-002.htm.
Recently, the CERT/CC has received reports of intruders using open mail relays to propagate malicious code such as the "Hybris Worm." For more information, please see CERT® Incident Note IN-2001-02 located at: http://www.cert.org/incident_notes/IN-2001-02.html.
A vulnerability in Domain Name System software is still being exploited.
A script that exploits the BIND INFOLEAK and TSIG vulnerability has been released. Please update your BIND server if you haven't already done so.
The CERT/CC has recently learned of four vulnerabilities spanning multiple versions of the Internet Software Consortium's (ISC) Berkeley Internet Name Domain (BIND) server. Because the majority of name servers in operation today run BIND, these vulnerabilities present a serious threat to the Internet infrastructure. For more information, please see CERT® Advisory CA-2001-02 located at: http://www.cert.org/advisories/CA-2001-02.html.

Viruses

HTML_SATANIK.B (Aliases: VBS/Loveletter@MM, VBS.Rewind.A@MM, SATANIK.B) (HTML Virus): A destructive HyperText Markup Language (HTML) virus that is written in Visual Basic Script (VBS). This virus overwrites many common file formats with its virus code. The virus is capable of propagating via MS Outlook, and it sends itself out once every 20 executions.

VBS_A24 (Aliases: VBS.a24, VBS/Netlog.worm.g, A24) (Visual Basic Script Worm): This Visual Basic Script (VBS) deletes files dropped by VBS_NETLOG. It attempts to map a specific drive, drive, X:\, to any machine connected on a network via Windows NetBIOS.

VBS/Carnival-A (Visual Basic Script Worm): This worm is received via an e-mail with the following details:

Subject: "Next Week: Brazilian Carnival"
Body: "That's Great..."
Attachment: Brazilian_Carnival.JPG.vbs

The worm attempts to copy itself to the TEMP directory. If it succeeds, it then sends a copy of itself to everyone in the Outlook address books.

VBS/Cuartel-A (Visual Basic Script Worm): This is a worm that spreads via Network drives. It copies itself to a file called "NAV.EXE***.VBS" (where *** represents 74 spaces) in the Windows temp folder. It then sets the registry to run that file. The virus changes the Internet Explorer home page to display a pornographic image and always disables IE's proxy settings. It also attempts to delete the associations in the registry for files with the extensions XLS, DOC and MDB. The worm spreads by overwriting files on remote drives with the extensions BTR, PST, XLS, MDB, JPG, PAB and WAB. Every time the worm is run it will attempt to send "C:\windows\explorer.exe" one thousand times to two people at "yrba.com.ar," using Outlook. Each message is deleted after being sent.

VBS/Kakworm-Z (Alias: Mid/Kakworm-Z) (Visual Basic Script Worm): This is a variant of the VBS/Kakworm worm. The worm will run if the user has Internet Explorer, Outlook or Outlook Express, but it will only spread to other users if Outlook Express 5.0 is used to send e-mail. Even if you receive an infected message, you cannot be affected unless you have an Internet Explorer based product installed. The worm arrives embedded in an e-mail message as the message HTML signature. The recipient of the message cannot see any visible symptoms as there is no displayable text in the signature. If the user opens or previews the infected e-mail message, the worm drops file BAP.HTA into the Windows start-up folder. BAP.HTA runs the next time Windows is started, creating the C:\WINDOWS\BAP.HTM file and changing the Microsoft Outlook Express registry settings so that the BAP.HTM is automatically included in every outgoing message as a signature. The BAP.HTA also changes the Windows registry to execute itself and sets the Internet Explorer home page to the member's page of www.ignifuge.com. Www.ignifuge.com is an advertising site whose members are rewarded if they persuade their friends/colleagues to visit the site.

VBS.Kidarcade (Visual Basic Script Worm and Java Script Virus): This virus is based on Visual Basic Script (VBS) and has been put into an HTML page, and is on at least one Web site. The virus installs a Backdoor Trojan that allows unauthorized access to the infected computer.

VBS.Oap@mm (Visual Basic Script Worm): VBS.Oap@mm is a worm that spreads by replying to all messages in the Microsoft Outlook inbox. The message that the worm sends is the same message that is in the inbox, but with the worm attached at the bottom.

VBS/Malpoc-A (Visual Basic Script Worm): This virus arrives in an e-mail message as an attachment "Read_Me_Legal_Notice.PDF.vbs." Once run, the worm will attempt to reply to every message in the Outlook Inbox. It will use the original subject and body text of each message adding the attachment "Read_Me_Legal_Notice.PDF.vbs."

VBS.Monde.A (Visual Basic Script Worm): VBS.Monde.A is an HTML file written in Visual Basic Script (VBS). If the infected HTML file is opened on the computer and Microsoft Word is installed, it inserts itself into all HTML files on drive C.

VBS.Sppst (Visual Basic Script Worm): The virus attempts to propagate by infecting files that have the .vbs extension and that are in the same folder as the virus. However, because this is the only way that this virus can propagate, it is highly unlikely that it will spread. The virus changes itself by inserting random comments between its own lines of code. Before attempting to infect a file, this virus checks for the comment "SPPST." If found, the virus will not infect the file. This appears to be an attempt to avoid infecting the same file multiple times.

VBS/Vierika-A (Visual Basic Script Worm): This worm has been reported in the wild. It is a VBS worm consisting of two parts. The first, a VB script, is likely to arrive as an attachment to an e-mail, in a file called VIERIKA.JPG.VBS. If run, this script changes the Internet Explorer home page to a page from web.tiscalinet.it and alters the Internet Explorer security settings. The second part of the worm is the HTML page at the address above. If the page is viewed after the worm has changed the IE security settings, a script will run which will create the file C:\VIERIKA.JPG.VBS. The worm will then attempt to e-mail this file as an attachment to addresses from the Outlook address book, with the e-mail subject line "Vierika is here" and the message body "Vierika.jpg."

VBS.XRA.A (Visual Basic Script Worm): This is a Visual Basic Script worm that uses an IRC client to spread. The worm copies itself to the following locations:

C:\Windows\System\XXXRATED.html.vbs
C:\Windows\System\RunDLL.vbs

If mIRC is installed on the system, it copies the Script.ini to the C:\Mirc folder. After infection, when mIRC is run it uses the Script.ini file to spread itself. The worm also attempts to overwrite doc, .txt, .vbs, .js, and .html files in the C:\My Documents folder

W32/Myba-A (Alias: I-Worm.Myba (Win32 Worm): This is an e-mail-aware worm which spreads using Microsoft Outlook. The worm sends e-mail messages to all contacts from your Outlook address book. The e-mail has the following characteristics:

Subject: My Baby pic !!!
Message text: Its my animated baby picture !!

If the attached file is run, it displays a pornographic animation of a baby boy and copies itself into the Windows system directory with the filenames WINKERNEL32.EXE, WIN32DLL.EXE, COMMAND.EXE, CMD.EXE and MYBABYPIC.EXE. The virus changes the Windows Registry keys \HKLM\Software\Microsoft\Windows\CurrentVersion\Run and HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices so that it automatically runs whenever Windows is started. The worm has several payloads that activate depending on the current date and time. It searches through the subdirectory tree and overwrite files with the extensions .C, .CPP, .CSS, .H, .HTA, .JS, .JSE, .PAS, .PBL, .SCT, and .WSH. New files are created with filenames identical to the overwritten file, but with a .EXE extension. A new file is created for every file with the MP2, MP3, and M3Uextenstion found, and the original file is changed so that the hidden attribute is set. The new filename is identical to the original filename but with the EXE extension added to the original one.

W32.Taz@mm (Win32 Worm): This is a worm written in Visual Basic. The worm can spread using mIRC, Pirch, and Microsoft Outlook. However, to function, this worm requires the Msbvm60.dll file. This is not a standard system file, and it is therefore not likely that this worm will execute on most Windows systems.

W97M.Coco.A (Word 97 Macro Virus): This is a stealth Word macro virus that infects the active document and the Normal.dot template.

W97M_TITCH.H (Alias: TITCH.H) (Word 97 Macro Virus): This macro virus infects the global template when an infected document is closed. It intercepts the auto macro AutoClose and avoids re-infecting the global template by searching for its virus module, "UPC116STAG." It uses the file UPC116STAG.TMP to export its virus code during infection and deletes it immediately afterward. When the global template is infected, any subsequent closing of Word documents causes the virus to infect active documents. It replicates, but has no destructive payload.

W97M.Turn.A (Word 97 Macro Virus): This is a macro virus that infects the Normal.dot template upon opening an infected document. It then infects documents when they are closed. This virus also disables the Visual Basic Editor.

W97M.Wu.A (Word 97 Macro Virus): This is a macro virus that poses as a Virus Inspector when it infects other documents. This virus infects documents when a clean document is opened. If the virus finds an older version of itself installed, it deletes the older version and replaces the code with itself.

WM97/E4 (Word 97 Macro Virus): On the 20th of any month, WM97/E4 will create the file C:\start.exe and run it. Start.exe is a copy of Joke/Win-Wobble.

WM97/Marker-GL (Word 97 Macro Virus): WM97/Marker-GL is a minor variant of the WM97/Marker-BN Word macro virus.

WM97/Metys-K (Word 97 Macro Virus): WM97/Metys-K is a minor variant of the WM97/Metys-D Word macro virus.

WM97/Metys-O (Word 97 Macro Virus): WM97/Metys-O is a Word macro virus. It has been created as the result of an interaction between the WM97/Class-D and WM97/Metys-I macro viruses but does not exhibit the same payload as WM97/Class-D.

WM97/Myna-AI (Word 97 Macro Virus): This is a variant of WM97/Myna-AF that does little more than replicate. It contains the phrase "This Document," which is used as a flag to check for the presence of the virus.

WM97/Myna-AJ (Word 97 Macro Virus): This is a minor variant of the WM97/Myna-J Word macro virus. It does little more than replicate and contains the phrase "MYNAMEISVIRUS," which is used as a flag to check for the presence of the virus.

WM97/WMVG-A (Alias: VBS/WMVG-A) (Word 97 Macro Virus): This virus is a Word macro virus created by a virus construction kit. On the 27th day of any month it will display a dialog box titled "ERAP PARIN" containing the text "ERAP Pa rin! GMA gahaman! Erap pa rin!" The virus also drops a Visual Basic Script, which attempts to reinfect computers.

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table starts with Trojans discussed in CyberNotes #2001-01, and items will be added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on Trojans and Trojan variants that anti-virus software detects. NOTE: At times, Trojans may contain names or content that may be considered offensive.

Trojan	Version	CyberNotes Issue #
Backdoor.Acropolis	N/A	CyberNotes-2001-04
Backdoor.Netbus.444051	N/A	CyberNotes-2001-04
Backdoor-JZ	N/A	CyberNotes-2001-02
BAT.Install.Trojan	N/A	CyberNotes-2001-04
BAT_DELWIN.D	**N/A**	**Current Issue**
BAT_EXITWIN.A	N/A	CyberNotes-2001-01
DLer20.PWSTEAL	**N/A**	**Current Issue**
Flor	N/A	CyberNotes-2001-02
HardLock.618	N/A	CyberNotes-2001-04
PHP/Sysbat	N/A	CyberNotes-2001-02
PIF_LYS	N/A	CyberNotes-2001-02
PWSteal.Coced240b.Tro	N/A	CyberNotes-2001-04
Troj/KillCMOS-E	N/A	CyberNotes-2001-01
TROJ_AOL_EPEX	N/A	CyberNotes-2001-01
TROJ_AOLWAR.B	N/A	CyberNotes-2001-01
TROJ_AOLWAR.C	N/A	CyberNotes-2001-01
TROJ_APS.216576	N/A	CyberNotes-2001-03
TROJ_AZPR	N/A	CyberNotes-2001-01
TROJ_BAT2EXEC	N/A	CyberNotes-2001-01
TROJ_BKDOOR.GQ	N/A	CyberNotes-2001-01
TROJ_BUSTERS	N/A	CyberNotes-2001-04
TROJ_DARKFTP	N/A	CyberNotes-2001-03
TROJ_DUNPWS.CL	**N/A**	**Current Issue**
TROJ_DUNPWS.CL	N/A	CyberNotes-2001-04
TROJ_FIX.36864	N/A	CyberNotes-2001-03
TROJ_GLACE.A	N/A	CyberNotes-2001-01
TROJ_GNUTELMAN.A	**N/A**	**Current Issue**
TROJ_GOBLIN.A	N/A	CyberNotes-2001-03
TROJ_GTMINESXF.A	N/A	CyberNotes-2001-02
TROJ_HERMES	N/A	CyberNotes-2001-03
TROJ_HFN	N/A	CyberNotes-2001-03
TROJ_ICQCRASH	N/A	CyberNotes-2001-02
TROJ_IF	**N/A**	**Current Issue**
TROJ_JOINER.15	N/A	CyberNotes-2001-02
TROJ_MOONPIE	N/A	CyberNotes-2001-04
TROJ_MYBABYPIC.A	**N/A**	**Current Issue**
TROJ_NAKEDWIFE	**N/A**	**Current Issue**
TROJ_NAVIDAD.E	N/A	CyberNotes-2001-01
TROJ_PARODY	**N/A**	**Current Issue**
TROJ_PORTSCAN	N/A	CyberNotes-2001-03
TROJ_QZAP.1026	N/A	CyberNotes-2001-01
TROJ_RUNNER.B	N/A	CyberNotes-2001-03
TROJ_RUX.30	N/A	CyberNotes-2001-03
TROJ_SUB7.21.E	**N/A**	**Current Issue**
TROJ_SUB7.401315	N/A	CyberNotes-2001-01

Trojan	Version	CyberNotes Issue #
TROJ_SUB7.MUIE	N/A	CyberNotes-2001-01
TROJ_SUB7.V20	N/A	CyberNotes-2001-02
TROJ_SUB7DRPR.B	N/A	CyberNotes-2001-01
TROJ_SUB7DRPR.C	N/A	CyberNotes-2001-03
TROJ_TPS	**N/A**	**Current Issue**
TROJ_TWEAK	N/A	CyberNotes-2001-02
TROJ_WEBCRACK	N/A	CyberNotes-2001-02
Trojan.MircAbuser	N/A	CyberNotes-2001-04
Trojan.Sheehy	**N/A**	**Current Issue**
VBS.Cute.A	**N/A**	**Current Issue**
VBS.Delete.Trojan	N/A	CyberNotes-2001-04
VBS.Trojan.Noob	N/A	CyberNotes-2001-04
W32.BatmanTroj	N/A	CyberNotes-2001-04

BAT_DELWIN.D (Alias: DELWIN.D): This batch file Trojan deletes *.EXE and *.COM files in the Windows directory. Thereafter, the deleted files must be restored manually or Win9x should be completely reinstalled.

DLer20.PWSTEAL: When run, DLer20.PWSTEAL copies itself to C:\Windows\System\Backup32.exe and runs memory-resident from that file. The original file that was opened is deleted. DLer20.PWSTEAL also adds the value Backup C:\WINDOWS\SYSTEM\BACKUP32.EXE to the following registry key: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run. This causes the Trojan to run when Windows starts.

TROJ_DUNPWS.CL (Aliases: DUNpws.cl, Trojan.PSW.TFC, HackTool.PWSteal, Troj/Zorro): This backdoor, password-stealing Trojan is a Windows executable program that attempts to crack dial-up networking passwords and save them in a file. Upon execution, it will access the victim's PC and send the password to the author. Activity of the virus cannot be seen on the PC, but it creates a named "~TF43C.TMP" text file.

TROJ_GNUTELMAN.A (Aliases: GNUTELMAN.A, MANDRAGORE, VBS/Gnutella, Gnuman.A, Gnutella Worm): This Trojan connects to a file sharing network, GNUTELLA, and disguises itself as a searched file in that network that allows it to spread to other users who download it. Upon execution, this Trojan attaches itself to a peer-to-peer, file-sharing network, GNUTELLA, via port 99. The Trojan node on the Gnutella network listens to the stream of traffic and returns a perfect result to every query. For example, if users on the network search on an MP3 file, this Trojan returns a result that exactly matches their query except that it sends an executable, *.EXE, file, which is a copy of this Trojan. If a user is running a Windows NT/2000 system, and downloads and executes the file, the Trojan installs itself as a service. If the user is running a Windows 9x/Me machine the Trojan attempts to install itself in the "Startup" folder. This Trojan drops a copy of itself as GSPOT.EXE file in Windows 9X /ME machines, and in C:\windows\Start menu\programs\startup and C:\Winnt\Profiles\<UserName>.000\StartMenu\ Programs\StartUp in Windows 2000/NTmachines.

TROJ_IF (Aliases: BackDoor-IF.svr, IF): This backdoor Trojan is similar to the BACK ORIFICE Trojan and the SUBSEVEN Trojan that allow remote users virtually unlimited access to an infected system. Upon execution, it drops an UNDLL.EXE file that is a key generator for a Nero v5.0.0.x program in the Windows directory of the infected system. The Trojan then replaces, with its own copy, a normal SYSTRAY.EXE file that is found in the system directory. It moves the original SYSTRAY.EXE to an Updates folder that it has created in the Windows system directory. The infected SYSTRAY.EXE is included in the system registry so that the Trojan is memory resident upon every bootup. When active in memory, it acts as a service so that it cannot be viewed in the Task Manager, or by pressing Ctrl-Alt-Del.

TROJ_MYBABYPIC.A (Aliases: MYBABYPIC.A, I-Worm.Myba, Backdoor.MyBabyPic): This Trojan propagates via MS Outlook as an EXE attachment and the subject line, "My Babypic." When the EXE file is executed, a message box with the picture of a child is displayed. When this message box is closed, the Trojan drops several copies of itself in the Windows\System directory and adds several registry entries to enable it to execute at each Windows start up. This Trojan needs Windows Scripting Host to function and upon execution tries to connect to a certain web site. In addition to this, the Trojan code also has some destructive payloads, which range from overwriting files with certain extensions to deleting certain files.

TROJ_NAKEDWIFE (Aliases: NAKEDWIFE, W32/Naked@MM, W32.HLLW.JibJab@mm): This destructive Trojan was written in Visual Basic Script and requires the presence of MSVBVM60.DLL in the infected computer's system directory to run. Upon execution, this Trojan deletes all DLL, INI, EXE, BMP, LOG and COM files in the Windows and system directories. Due to this, it is impossible to reboot an infected system. It propagates via MS Outlook and Outlook Express, by sending out an e-mail to every e-mail address listed in the infected user's address book. This e-mail has the subject line "FW: Naked Wife" and the attachment "NakedWife.EXE.”

TROJ_PARODY: This Win32 Trojan adds text files with odd names and corrupts selected files in an infected system. It attempts to format drive C: upon next boot up.

Trojan.Sheehy (Alias: Trojan.Sheeby.bat): This is a very damaging Trojan horse program that depends on the current environment such as system date and time. Trojan.Sheehy may create a copy of itself as the file Ramsys.exe in the \Windows\System folder. It modifies Win.ini file by adding the text: C:\WINDOWS\SYSTEM\RAMSYS.EXE to the load= line (NOTE: If Windows is installed in a different location, the path will differ.) It then modifies the Autoexec.bat file, and adds the line:

```
            IF NOT EXIST C:\WINDOWS\SYSTEM\RAMSYS.EXE DELTREE /Y C:
```

This instructs the system to delete the entire contents of the hard disk if the Ramsys.exe is ever deleted or renamed. The Trojan horse may also choose at random an executable program that is located in the \Windows\System folder, and replace it with a copy of itself.

TROJ_SUB7.21.E (Alias: SUB7.21.E): This Win32 Trojan is one of several versions of the notorious backdoor hacking tool, TROJ_SUB7. This server-side hacking tool allows a remote hacker access to an infected computer. It is also similar to the Back Orifice Trojan that compromises network security. It gives system administrator privileges to a remote user via the infected system's Internet link. The icon of this Trojan resembles that of an MPEG file when viewed in Windows Explorer.

TROJ_TPS (Aliases: TPStrojan.e, TPS, Trojan.Win32.TPS): This is a clean up program for an application log file generated by a Trojan, upon execution. It uses a filename SYSTEM32 and spawns this program before it terminates. It has no destructive payload.

VBS.Cute.A: This is a Trojan horse written in Visual Basic Script (VBS). When you receive it, it appears to be hard disk drive benchmark software named Cutie. If the Trojan horse is executed, it overwrites all .exe, .com, and .dll files on your system.